U.S. Department of Justice

United States Attorney
Eastern District of New York

AFM:EHS/AA
F. #2022R00315

271 Cadman Plaza East
Brooklyn, New York 11201

May 23, 2025

By ECF and E-mail

The Honorable Frederic Block
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Nicholas Ceraolo
Criminal Docket No. 23-CR-236 (FB)

Dear Judge Block:

The government respectfully submits this letter in advance of the defendant Nicholas Ceraolo's sentencing, which is scheduled for May 30, 2025. The defendant pleaded guilty to Counts One and Two of the indictment, charging violations of 18 U.S.C. § 371 (Conspiracy to Commit Computer Intrusions) and 18 U.S.C. § § 1028A(a)(1), (b), and (c)(4) (Aggravated Identity Theft). [1] *See* PSR ¶¶ 1–2. For the reasons stated below, the government respectfully requests a sentence within the Guidelines range of 30 to 36 months' imprisonment.

I. Factual Background

A. "ViLE"

The defendant and co-defendant Sagar Singh were members of "ViLE," a cybercriminal organization. PSR ¶ 7. Members of ViLE conspired to illegally obtain victims' personal information and maliciously used it to harass, threaten, or extort victims. *Id.* ViLE's logo is a girl being hanged (PSR ¶ 10), pictured below. The defendant's nickname ("Ominous") appears under the picture:

[1] The information below is taken from the United States Probation Department ("Probation") Presentence Investigation Report ("PSR") dated April 25, 2025 and other evidence gathered as part of the investigation and prosecution of the defendant.

ViLE members, including the defendants, used various sophisticated methods to obtain victims' personal information, including by submitting fraudulent legal process to social media companies to get user registration information. PSR ¶ 8. The defendants also co-opted and corrupted corporate insiders, searched public and private online databases, and, as charged in the instant indictment, accessed a nonpublic United States government database without authorization and unlawfully used official email accounts belonging to law enforcement officers in other countries. *Id*.

After obtaining victim information, the defendants posted it on an online forum ("Forum-1"), administered by the leader of ViLE, an unindicted co-conspirator who lives abroad. PSR ¶ 9. Victims were then extorted into paying a ransom, or surrendering access to their social media accounts, in exchange for ViLE members removing their personal information from Forum-1. *Id*.

B. The Defendant Breached a Secure Government Database

In May 2022, the defendants conspired to access a nonpublic portal maintained by a United States federal law enforcement agency (the "Federal Law Enforcement Agency") without authorization, thereby obtaining confidential, restricted information. *See* PSR ¶ 11–15. Specifically, defendant Ceraolo unlawfully used a law enforcement officer's stolen password to access the nonpublic, password-protected online portal ("the Portal") for federal law enforcement use only. *Id*. Access to the Portal was restricted to law enforcement officials. *See* PSR ¶ 11. Any user who entered the Portal had to view and clicked through multiple warning screens, including a warning that "unauthorized use or access to [the] system may subject you to criminal and/or civil prosecution and penalties," before proceeding. PSR ¶ 12.

The Portal was utilized for confidential law enforcement functions, including sharing intelligence between law enforcement agencies and maintaining nonpublic records of narcotics and currency seizures. *See* PSR ¶ 11–12. The Portal also was used for storing and maintaining law enforcement intelligence reports. PSR ¶ 11. After gaining unauthorized access

to the Portal, Ceraolo acknowledged knowing that his conduct was criminal. PSR ¶ 15. After Singh sent Ceraolo the stolen login credentials, Ceraolo responded: "It worked… this is a[] [Federal Law Enforcement Agency] agent pretty sure . . . were all gonna get raided one of these days i swear." *Id*.

Records from online platforms indicate that Ceraolo shared the stolen credentials belonging to a law enforcement officer with online associates, including fellow ViLE members. PSR ¶ 17. Ceraolo and an associate discussed how to "scrape" data from the Portal, which refers to using automated tools to export voluminous information from the website into a local file. *Id*. In this conversation, Ceraolo also demonstrated his knowledge by describing the Portal as an "intel center for [Federal Law Enforcement Agency]." *Id*.

C. The Defendant Fraudulently Posed as Law Enforcement

Between February 2022 and May 2022, Ceraolo also used hacked email addresses belonging to victims to impersonate law enforcement in order to obtain personal victim information. PSR ¶ 19. Specifically, Ceraolo used, without authorization, an email account belonging to a Bangladeshi police official to communicate with U.S.-based social media platforms, purporting to be a police officer contacting the providers from an official police account. *Id*. Under the false pretext that platform users were committing crimes or in life-threatening danger, Ceraolo requested the personal information of these users. *Id*. Accordingly, Ceraolo induced and attempted to induce platforms to provide their users' private information, which the platforms would not have otherwise provided. *Id.* By this means, Ceraolo successfully fraudulently obtained victim subscriber and user information from multiple social media platforms. *Id*.

II. Applicable Law

The Supreme Court has explained that "a district court should begin all sentencing proceedings by correctly calculating the applicable the United States Sentencing Guidelines ("U.S.S.G." and "Guidelines") range. *Gall v. United States*, 552 U.S. 38, 49 (2007). Though advisory, *see United States v. Booker*, 543 U.S. 220, 264 (2005), the Guidelines nonetheless are "the starting point and the initial benchmark," *Gall*, 552 U.S. at 49; *see also Molina-Martinez v. United States*, 578 U.S. 189, 198–99 (2016) (explaining that "[t]he Guidelines are the framework for sentencing and anchor the district court's discretion" (alternation and internal quotation marks omitted)).

After calculating the applicable Guidelines range, the court must consider the factors outlined in § 3553(a), *see Gall*, 552 U.S. at 49, and impose a sentence "sufficient, but not greater than necessary to fulfill the purposes of sentencing," *United States v. Cavera*, 550 F.3d 180, 188 (2d Cir. 2008) (citing 18 U.S.C. § 3553(a)(2)). Section 3553(a) directs the court "in determining the particular sentence to impose" to evaluate: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the statutory purposes noted above; (3) the kinds of sentences available; (4) the kinds of sentence and the sentencing range as set forth in the Sentencing Guidelines; (5) the Sentencing Guidelines policy statements; (6) the need to

avoid unwarranted sentencing disparities; and (7) the need to provide restitution to any victims of the offense.

Although the Guidelines are no longer mandatory, they continue to play a critical role in trying to achieve the "basic aim" that Congress sought to meet in enacting the Sentencing Reform Act, namely, "ensuring similar sentences for those who have committed similar crimes in similar ways." *Booker*, 543 U.S. at 252. "[I]n the ordinary case, the Commission's recommendation of a sentencing range will reflect a rough approximation of sentences that might achieve § 3553(a)'s objectives." *Kimbrough v. United States*, 552 U.S. 85, 109 (2007) (citation and internal quotation marks omitted). Indeed, the Supreme Court has held that, on appeal, a Guidelines sentence may be presumed to be reasonable because "the sentencing statutes envision both the sentencing judge and the [Sentencing] Commission as carrying out the same basic § 3553(a) objectives." *Rita v. United States*, 551 U.S. 338, 358 (2007). "An individual judge who imposes a sentence within the range recommended by the Guidelines thus makes a decision that is fully consistent with the Commission's judgment in general." *Id.* at 350. Furthermore, sentences within the applicable Guidelines promote Congress' goal in enacting the Sentencing Reform Act: "to diminish unwarranted sentencing disparity." *Id.* at 354.

At sentencing, "the court is virtually unfettered with respect to the information it may consider." *United States v. Alexander*, 860 F.2d 508, 513 (2d Cir. 1988). Indeed, "[n]o limitation shall be placed on the information concerning the background, character, and conduct of a person convicted of an offense which a court of the United States may receive and consider for the purpose of imposing an appropriate sentence." 18 U.S.C. § 3661.

III. Guidelines

The Guidelines calculation detailed in the PSR is incorrect as further described below. The correct Guidelines range of imprisonment is 30 to 36 months' imprisonment. Count 1 carries a 6-12 months' imprisonment Guidelines range. Count 2 carries a mandatory minimum sentence of 24 months' imprisonment.

A. The Applicable Guidelines Range

The appropriate Guidelines calculation is set forth below:

Base Offense Level (U.S.S.G. § 2X1.1 & 2B1.1(a)(2))		6
Plus:	Offense Involved Sophisticated Means (U.S.S.G. § 2B1.1(b)(10)(C))	+2
Plus:	Offense Involved Misrepresentation Acting on Behalf of Government (U.S.S.G. § 2B1.1(b)(9))	+2
Plus:	Offense Involved Dissemination of Personal Information (U.S.S.G. § 2B1.1(b)(18))	+2

Plus:	Offense Involved a Computer System Used By Government In Furtherance of The Administration of Justice (U.S.S.G. § 2B1.1(b)(19)(A)(i))	+2
Less:	Adjustment for certain zero-point offenders (U.S.S.G. § 4C1.1)	-2
Total:		12

Probation correctly calculated the base level offense of 6 and applied the sophisticated means enhancement (PSR ¶¶ 36-37) , arriving at a total offense level of 12, after application of U.S.S.G. § 2B1.1(b)(10)(C) (adjusting the offense level to 12 if it would otherwise be less than 12). PSR ¶ 37.

The government disagrees, however, with Probation's calculation of the total offense level, because it fails to account for several applicable enhancements: U.S.S.G. § 2B1.1(b)(9)(a) (Offense Involved Misrepresentation Acting on Behalf of Government); U.S.S.G. § 2B1.1(b)(18) (Offense Involved Dissemination of Personal Information); and U.S.S.G. § 2B1.1(b)(19)(A)(i) (Offense Involved a Computer System Used By Government In Furtherance of The Administration of Justice). For the reasons that follow, each of these enhancements is applicable and the Court should find that they all apply.

First, the defendant falsely represented that he was acting on behalf of a government entity. He used, without authorization, an email account belonging to a Bangladeshi police official to communicate with U.S.-based social media platforms, purporting to be a police officer contacting the providers from an official police account. PSR ¶ 19. The Second Circuit has affirmed the application of § 2B1.1(b)(9)(a) where the defendant posed as law enforcement. *See United States v. Nieves*, 727 F. App'x 721, 724 (2d Cir. 2018) (affirming district court's application of § 2B1.1(b)(9)(a) where defendant misrepresented himself as a "federal immigration officer" with the power to help his victims obtain lawful immigration status in return for payment of bribes). Accordingly, the Court should apply § 2B1.1(b)(9)(a).

Second, the offense involved dissemination of personal information. As described above, ViLE members, including the defendant and his codefendant, used various sophisticated methods to obtain victims' personal information. PSR ¶ 8. After obtaining victim information, ViLE members posted it on Forum-1 and extorted victims. Based on these facts, the Court should apply U.S.S.G. § 2B1.1(b)(18).

Third, the offense involved a computer system used by government in furtherance of the administration of justice. The term "government entity" includes the "Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country." 18 U.S.C. § 1030. Here, the government entity is the federal law enforcement agency which operates the

Portal. Specifically, defendant Ceraolo unlawfully used a law enforcement officer's stolen password to access the nonpublic Portal. Access to the Portal was restricted to law enforcement officials (PSR ¶ 11) and used for law enforcement. As such, the Court should find that U.S.S.G. § 2B1.1(b)(19)(A)(i) applies.

An offense level of 12 carries a Guidelines range of 6-12 months. Under the grouping analysis, the defendant's total Guidelines is 30-36 months' imprisonment.

IV. Defendant Objections

A. Various Factual Objections

In a letter dated May 9, 2025, the defendant objects to the characterization that he was a member of the "cybercriminal group, known to its members as 'ViLE.'" Ltr. 1. The defendant claims—without citation to any evidence—that he was "not a member of" ViLE, and had "no knowledge or participation with this group." *Id.*; *see also* Ltr. 2 (objecting to paragraph eight on the ground that Ceraolo "was not a member of the group").[2]

These claims are inaccurate. Statements by Ceraolo and his co-conspirators confirm that the defendant was a member of ViLE, communicated with its leader and was familiar with its members, purpose, and criminal activities. For example, in a recorded May 17, 2022 interview with law enforcement conducted at his residence, the defendant described multiple successful and attempted episodes of computer hacking and identity theft that he undertook with other ViLE members or knew that they had undertaken. In a June 10, 2022 recorded interview, also conducted at his residence, the defendant described ViLE's mission, and how it had evolved from doxing to misuse of government emails. The defendant also described ViLE's internal group chat. The defendant's claim to have had "no knowledge or participation" in ViLE is false.

Ceraolo also demonstrated his familiarity with ViLE's extortionate platform, Platform-1. In the May 17, 2022 interview, the defendant identified the operators of Platform-1 and their various responsibilities, including an individual who was in charge of posting and removing extortionate content.

The record also shows that Ceraolo took part in various cybercrime schemes, including providing a ViLE member with IP addresses for a hacking attack, logging into a law enforcement email account and sending fraudulent subpoenas and emergency disclosure requests to various internet providers, and trading credentials with other ViLE members. It is simply not

[2] The defendant also emphasizes that "[h]e never left the living room of his house in connection with this matter." Ltr. 1. This is irrelevant. Conspiracy to commit computer intrusion and aggravated identity theft require no in person meetings—these are crimes that can be (and often are) committed exclusively from a computer.

true that "[a]ll Mr. Ceraolo did was access a nonpublic US government database without authorization," nor is it true that the defendant's conduct is victimless. Ltr. 2.

For these reasons, the defendant's attempts to distance himself from ViLE and his co-conspirators' activities should be rejected. The defendant knew about and participated in ViLE's various cybercrime activities, as described above. The Court should overrule the defendant's objections to paragraphs seven through 14. Ltr. 1-2.

B. Minor Role Adjustment

Ceraolo also seeks a minor role adjustment. Ltr. 2. Because the defendant cites no evidence in support of his request (and because there is no such evidence in any event), the Court should overrule the objection.

Section 3B1.2 of the Sentencing Guidelines provides for a two-level downward adjustment where the defendant was a "minor participant." The commentary to the Guidelines provides that a defendant is a "minor participant" where he is "less culpable than most other participants in the criminal activity." In assessing a defendant's role, the court should consider "the nature of the defendant's relationship to other participants, the importance of the defendant's actions to the success of the venture, and the defendant's awareness of the nature and scope of the criminal enterprise." *United States v. Wynn*, 108 F.4th 73, 81 (2d Cir. 2024). Notably, "it is the defendant who bears the burden of establishing his entitlement to that reduction by a preponderance of the evidence." *Id*. at 80. "A sentencing court is not bound to accept a defendant's self-serving characterizations of his role in an offense." *Id*. at 82.

As described above, Ceraolo was a member of ViLE, knew its objectives, and participated in its various cybercrime activities, including trading credentials for and logging into U.S. law enforcement databases, helping identify hacking targets, and submitting fraudulent subpoenas to internet providers. PSR ¶¶ 7-24. He did not have diminished knowledge, participation, or culpability with respect to ViLE's activities.

C. Downward Departure for Reduced Mental Capacity

The defendant also fails to meet his burden in establishing a downward departure for "significantly reduced mental capacity." A defendant has "significantly reduced mental capacity" when the defendant "has a significantly impaired ability to ... control behavior that the defendant knows is wrongful." U.S.S.G. § 5K2.13 cmt. n. 1. A court may depart on this basis as long as the defendant "demonstrates, by a preponderance of the evidence," that (1) he suffered from a significantly diminished capacity and (2) there is "a causal link between that reduced capacity and the commission of the charged offense." *United States v. Kim*, 313 F. Supp. 2d 295, 297–98 (S.D.N.Y. 2004) (citing *United States v. Prescott*, 920 F.2d 139, 145 (2d Cir. 1990)).

The defendant cannot meet his burden on either ground. As to the first element, he is not suffering from significantly reduced mental capacity. The defense report by Dr. Kanishk Solanki describes the defendant as having "issues with social interactions," which he finds

"consistent with Autism Spectrum Disorder," and further adds that Ceraolo "mentioned some depressive symptoms in and around the time of the instant offenses." Solanki Report at 8. Without minimizing challenges the defendant may face, these conditions cannot be fairly described as resulting in a "significantly reduced mental capacity." *See United States v. Greenfield*, 244 F.3d 158, 162 (D.C. Cir. 2001) ("A diagnosis of depression, alone, does not establish that a defendant suffered from 'significantly reduced mental capacity' under § 5K2.13."); Christine N. Cea, Autism and the Criminal Defendant, 88 St. John's L. Rev. 495, 522 (2014) (noting that "autism is not a factor that allows for a downward departure").

As to the second element, the defendant cannot demonstrate a causal link between his purportedly reduced capacity and the offense conduct. Even if the Court were to decide that autism spectrum disorder or self-reported depression could in some circumstances lead to significantly reduced mental capacity, those disorders are collateral to the charged conduct of this defendant. Nothing in Ceraolo's submissions, or the report of Dr. Solanki, persuasively connect his condition to the offense conduct. To the contrary, the defendant's trading and use of login credentials to a U.S. government database, extended engagement in online activity, development and execution of complex technical tasks, and ongoing participation in the conduct reflect planning and cognitive control. Courts routinely find that such complex or structured behavior weighs against a finding of significantly reduced capacity. *See United States v. Withers*, 100 F.3d 1142, 1148 (4th Cir. 1996) (defendant ineligible for downward departure because she failed to show that her depression rendered her unable to process information or to reason; she was fully capable of following a complex set of instructions to transport heroin successfully into the United States); *Kim*, 313 F. Supp. 2d 299 (rejecting downward departure for reduced capacity where defendant suffered from compulsive disorder but the disorder did not cause the defendant to forge checks and commit fraud). In other words, while depression and autism may have led the defendant to retreat to his computer, they did not compel or cause him to use that computer for cybercrime.

V. The Section 3553(a) Factors Demand a Substantial Term of Incarceration

As explained in greater detail below, a substantial sentence of incarceration is warranted given the nature and seriousness of the defendant's criminal offenses, the requirement to promote respect for the law, and the need for both general and specific deterrence. *See* 18 U.S.C. § 3553(a). For these reasons, the government respectfully submits that a Guidelines sentence of imprisonment of 30 to 36 months is sufficient, but not greater than necessary, to satisfy the goals of sentencing. *Id.*

A. Nature and Circumstances of the Offense

The defendant perpetrated a complex cybercrime and identity theft conspiracy that warrants a substantial penalty. His criminal conduct was serious in nature and broad in scope. Utilizing his resources and contacts through his membership in the cybercriminal group "ViLE," Ceraolo inflicted substantial harm on various victims, including social media platform providers and federal law enforcement officers and agencies. Ceraolo violated data privacy, undermined the integrity of highly confidential information, took advantage of custodians of private customer

records, and compromised the security of a federal law enforcement database and highly sensitive intelligence materials.

Ceraolo also committed his crimes using sophisticated and exploitative means. The defendant's actions were deliberate—they exploited personal victim information and confidential federal law enforcement intelligence. Ceraolo also exploited companies' trust in government officials and government-issued subpoenas and took advantage of their commitment to public safety, inducing them to provide the private information of their users.

Data privacy impacts every citizen, agency, company, and institution in the United States. Social media platforms and providers, in particular, retain and safeguard a trove of private information that is not, and ought not to be, accessible to the public. A threat actor who knowingly penetrates these sensitive systems and databases, without authorization, poses a threat to any account holder, officer or otherwise. Similarly, the ability of law enforcement to confidentially and securely conduct criminal investigations and generate and store intelligence materials is of paramount importance.

B. General and Specific Deterrence

Given that criminal conduct like the defendant's is highly complex and typically difficult to detect and prosecute, principles of general deterrence warrant a substantial penalty. *See, e.g.*, *Harmelin v. Michigan*, 501 U.S. 957, 988-89 (1991) (noting that "since deterrent effect depends not only upon the amount of the penalty but upon its certainty, crimes that are less grave but significantly more difficult to detect may warrant substantially higher penalties"). Because internet and fraud-based crimes are more rational, cool and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence. *See United States v. Zukerman*, 897 F.3d 423, 429 (2d Cir. 2018) ("Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expected benefits of a crime and hence the punishment required to deter it.") (quoting *United States v. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994)); *see also United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006).

Here, a Guidelines sentence will help to deter Ceraolo, other ViLE members, and cybercriminals at large, who believe that they can generate income through computer intrusion, identity theft, social engineering, and fraudulent schemes against data providers and law enforcement agencies. Such persons should know that deceiving data providers into handing over private subscriber information, penetrating law enforcement databases, and unlawfully intercepting government intelligence, will result in a substantial term of custody. In addition, the nature of cybercrime activity generally renders it more difficult to uncover: cybercriminals engaged in computer intrusion and identity theft often utilize their technological advantage and fluency in online systems to cover the tracks of their digital footprints, obfuscate their identities, and evade law enforcement detection.

Additionally, computer intrusions, identity theft, and cyberattacks are extremely prevalent and ever-growing. The Federal Bureau of Investigation's Internet Crime Complaint

Center ("IC3") has calculated that in 2024 alone, internet crimes exceeded $16 billion in losses—a 33% increase in losses from the prior year. *See* Fed. Bureau of Investigation, Internet Crime Complaint Ctr., 2024 IC3 Annual Report (2024), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (last visited May 16, 2025). According to this same report, the top three most prevalent internet crimes of 2024 were email phishing, extortion, and personal data breach, all of which are relevant or directly applicable to ViLE's activities and Ceraolo's specific conduct: namely, hacking a Bangladeshi police official's email to contact companies and obtain private data, using "doxing" as a form of extortion, and exploiting stolen credentials, respectively. *See id*. Additionally, according to IC3's report, identity theft, computer intrusion (or "hacking") and government impersonation are also extremely prevalent and responsible for substantial financial loss annually. *See id*. Identity theft and computer intrusion in particular permeate various kinds of cyberattacks and cyber-enabled financial fraud, including the crimes in question, and government impersonation is the means Ceraolo used to fraudulently issue a subpoena and obtain subscriber information.

The defendant also needs to be specifically deterred. Ceraolo was an active member of an advanced cybercrime group that is dedicated to illicitly obtaining victims' personal information and using that data to "dox" victims through exposing their personal data, until they pay or surrender their social media account credentials as ransom. ViLE hacked into law enforcement databases, deliberately accessed and stole sensitive personal information, and leveraged this information to control its victims through threats and harassment. The defendant gained unauthorized access to a federal law enforcement database using the stolen credentials of a police officer, shared the police officer's stolen credentials with online associates, including another member of ViLE, and discussed with his associates how to "scrape" data from the Portal. Ceraolo also hacked into a different police official's email to forge a subpoena and induce online platform providers to provide victim's subscriber information. The harm that Ceraolo caused to victims and institutions was calculated, multilayered, unrelenting, and rooted in deception and exploitation. Accordingly, a Guidelines sentence would serve the interests of accountability, public safety, data privacy, and cybersecurity. Under these circumstances, the requested sentence is sufficient, but not greater than necessary, to achieve the goals of sentencing.

VI. Conclusion

For the reasons set forth above, the government respectfully requests that the Court impose a Guidelines sentence.

Respectfully submitted,

JOSEPH NOCELLA, JR.
United States Attorney

By: /s/
Alexander F. Mindlin
Ellen H. Sise
Adam Amir
Assistant U.S. Attorneys
(718) 254-7000

cc: Clerk of the Court (FB) (by ECF)
Defense Counsel of Record (by ECF and email)
U.S. Probation Officer (by email)